73. (New) One or more computer-readable media as recited in claim 72, wherein the state of a central processing unit comprises instructions and data residing in any caches and buffers of the central processing unit.

74. (New) One or more computer-readable media as recited in claim 72, wherein the state of a central processing unit comprises instructions and data residing in any registers of the central processing unit.

75. (New) A memory controller as recited in claim 46, wherein the controller is to reset the processor by clearing a state of the processor.

A1

76. (New) A memory controller as recited in claim 75, wherein the clearing the state of the processor comprises clearing all instructions and data from any caches or buffers of the processor.

77. (New) A memory controller as recited in claim 46, wherein the controller is to reset the processor by asserting, on a processor bus, a reset signal to the processor.

78. (New) A memory controller as recited in claim 77, wherein the reset signal comprises RESET#.

79. (New) An apparatus as recited in claim 57, wherein the reset signal clears a state of the processor.

80. (New) An apparatus as recited in claim 79, wherein the state of the processor includes instructions and data residing in any caches or buffers of the processor.

81. (New) An apparatus as recited in claim 57, wherein the processor reset portion is to assert the reset signal on a processor bus.

82. (New) An apparatus as recited in claim 57, wherein the reset signal comprises RESET#.

A1

83. (New) A computer as recited in claim 66, wherein the memory controller is further configured to reset the processor by clearing a state of the processor.

84. (New) A computer as recited in claim 83, wherein the state of the processor includes instructions and data residing in any caches and buffers of the processor.

85. (New) A computer as recited in claim 83, wherein the state of the processor includes instructions and data residing in any registers of the processor.

86. (New) A computer as recited in claim 66, wherein the memory controller is further configured to reset the processor by asserting, on a processor bus, a reset signal to the processor.

87. (New) A computer as recited in claim 66, wherein the memory controller is further configured to reset the processor by asserting a RESET# signal to the processor.

A1

88. (New) A method comprising:

allowing operation of a computer to begin based on untrusted code;

loading, under control of the untrusted code, a trusted core into memory of the computer;

preventing each of one or more central processing units and each of one or more bus masters in the computer from accessing the memory;

clearing a state of each of the one or more central processing units;

allowing one central processing unit to access the memory and execute trusted core initialization code to initialize the trusted core; and

after execution of the trusted core has been initialized, allowing any other central processing units and any bus masters in the computer to access the memory.

89. (New) A method as recited in claim 88, wherein the preventing comprises preventing each of the one or more central processing units and each of the one or more bus masters from accessing the memory in response to an

initialize trusted core command received from one of the one or more central processing units.

90. (New) A method as recited in claim 88, wherein the state of a central processing unit comprises instructions and data residing in any caches and buffers of the central processing unit.

A1 concl.

91. (New) A method as recited in claim 88, wherein the state of a central processing unit comprises instructions and data residing in any registers of the central processing unit.